THE CACCETTA-HÄGGKVIST CONJECTURE AND ADDITIVE NUMBER THEORY

MELVYN B. NATHANSON

Abstract. The Caccetta-Häggkvist conjecture states that if G is a finite directed graph with at least n/k edges going out of each vertex, then G contains a directed cycle of length at most k. Hamidoune used methods and results from additive number theory to prove the conjecture for Cayley graphs and for vertex-transitive graphs. This expository paper contains a survey of results on the Caccetta-Häggkvist conjecture, and complete proofs of the conjecture in the case of Cayley and vertex-transitive graphs.

1. Many edges imply short cycles

A *finite directed graph* $G = (V, E)$ consists of a finite set $V = V(G)$ of vertices and a finite set $E = E(G)$ of edges, where an edge $e = (v, v')$ is an ordered pair of vertices. If $e = (v, v')$ is an edge, then the vertex v is called the *tail* of e, and v' is called the *head* of e. The *outdegree* of a vertex $v \in V$, denoted $\mathrm{outdeg}_G(v)$, is the number of edges $e \in E$ of the form (v, v'), that is the number of edges with tail v. The *indegree* of a vertex $v' \in V$, denoted $\mathrm{indeg}_G(v')$, is the number of edges $e \in E$ of the form (v, v'), that is the number of edges with head v'.

Let v and v' be distinct vertices of the finite directed graph G. A *directed path of length* ℓ in G from vertex v to vertex v' is a sequence of ℓ edges

$$(v_0, v_1), (v_1, v_2), \ldots, (v_{\ell-1}, v_\ell)$$

such that $v = v_0$ and $v' = v_\ell$. A *directed cycle of length* ℓ in G is a sequence of ℓ edges $(v_0, v_1), (v_1, v_2), \ldots, (v_{\ell-1}, v_\ell)$ such that $v_0 = v_\ell$. A *loop* is a cycle of length 1, that is, an edge of the form (v, v). A cycle of length 2 is called a *digon*, and consists of two edges of the form (v_0, v_1) and (v_1, v_0), where $v_0 \neq v_1$. A *directed triangle* is a cycle of length 3 of the form $(v_0, v_1), (v_1, v_2), (v_2, v_0)$, where the vertices v_0, v_1, v_2 are distinct.

It is reasonable to expect that a finite directed graph with many edges should have many cycles, and, in particular, should have short cycles. A quantitative expression of this intuition is the following:

2000 *Mathematics Subject Classification.* 05C20,05C25,11B13,11P99.

Key words and phrases. Caccetta-Haggkvist conjecture, Cayley graph, vertex-transitive graph, Sidon sets, additive number theory.

This is the text of two talks in the New York Number Theory Seminar on February 9 and February 16, 2006. These notes are based on lectures by Matt DeVos and others at the American Institute of Mathematics (AIM) workshop on the Caccetta-Häggkvist conjecture in Palo Alto on Janaury 30-February 3, 2006, and on discussions with several conference participants. I wish to thank AIM for sponsoring this workshop.

The work of M.B.N. is supported in part by grants from the NSA Mathematical Sciences Program and the PSC-CUNY Research Award Program.

> There is a function $f(r)$ such that if G is a finite directed graph with n vertices and if there are at least r edges going out of every vertex in G, then G contains a cycle of length at most $f(r)n$.

A theorem of Chvátal-Szemerédi [4] shows that this is true with $f(r) = 2/(r+1)$. We start with a simple averaging argument.

Lemma 1. *Let $G = (V, E)$ be a finite directed graph such that $outdeg_G(v) \geq r$ for every $v \in V$. There exists a vertex $v_0 \in V$ such that $indeg_G(v) \geq r$.*

Proof. Suppose that every vertex of G has outdegree at least r. The number of edges $|E|$ satisfies the inequality

$$|V|r \leq \sum_{v\in V} \text{outdeg}_G(v) = |E| = \sum_{v\in V} \text{indeg}_G(v) \leq |V| \max\{\text{indeg}_G(v) : v \in V\}$$

and so there exists a vertex $v_0 \in V$ such that $\text{indeg}_G(v_0) \geq r$. □

Theorem 1 (Chvátal-Szemerédi)**.** *Let r be a positive integer. If $G = (V, E)$ is a finite directed graph with $|V| = n \geq r$ vertices such that $outdeg_G(v) \geq r$ for all $v \in V$, then G contains a cycle of length at most $2n/(r+1)$*

Proof. The proof is by induction on n. If $n = r$, then G is the complete directed graph on n vertices and contains a loop at each vertex. Let $n \geq r+1$ and assume that the Theorem holds for all graphs with less than n vertices. The number $|E|$ of edges in the graph satisfies the inequality

$$r|V| \leq \sum_{v\in V} \text{outdeg}_G(v) = |E| = \sum_{v\in V} \text{indeg}_G(v)$$

and so there is a vertex $v_0 \in V$ such that $\text{indeg}_G(v_0) \geq r$. Let A denote the set of vertices $a \in V$ such that $(a, v_0) \in E$ and let B denote the set of vertices $b \in V$ such that $(v_0, b) \in E$. If $v_0 \in A \cup B$, then (v_0, v_0) is an edge and so G contains a loop, that is, a cycle of length 1. Similarly, if $v_0 \notin A \cup B$ and $A \cap B \neq \emptyset$, then there is a vertex $v \in V$ such that (v_0, v) and (v, v_0) are both edges in G and so G contains a digon, that is, a cycle of length $2 \leq 2n/(r+1)$. Therefore, we can assume that the sets A, B, and $\{v_0\}$ are pairwise disjoint.

Since $|A| \geq r$ and $|B| \geq r$, it follows that $n \geq 2r+1$ and

$$\frac{2n}{r+1} \geq \frac{4r+2}{r+1} \geq 3.$$

Let $b \in B$ and let (b, v) be an edge in E. If $v = a \in A$, then (v_0, b), (b, a), and (a, v_0) is a directed triangle in G, that is, a cycle of length $3 \leq 2n/(r+1)$. Therefore, we can also assume that $v \notin A$ for every edge $(b, v) \in E$.

Let $v \in V \setminus (A \cup \{v_0\})$. Let d_A denote the number of edges in E of the form (v, a) with $a \in A$, let d_B denote the number of edges in E of the form (v, b) with $b \in B$, and let d_C denote the number of edges in E of the form (v, v') with $v' \notin A \cup B$. Since $(v, v_0) \notin E$, it follows that

$$d_A + d_B + d_C = \text{outdeg}_G(v) \geq r.$$

Let $d' = \min(d_A, |B| - d_B)$. Choose vertices $b_1, b_2, \ldots, b_{d'} \in B$ such that $(v, b_i) \notin E$ for $i = 1, \ldots, d'$, and let

$$E'(v) = \{(v, b_i) : i = 1, \ldots, d'\}.$$

An ordered pair in the set $E'(v)$ will be called a "new edge." Note that if $v \in B$, then $d_A = 0$ and $E'(v) = \emptyset$.

We construct a new graph $G' = (V', E')$ as follows. Let
$$V' = V \setminus (A \cup \{v_0\}.$$
Then
$$n' = |V'| = |V| - |A| - 1 \leq n - r - 1.$$
Let
$$E_0' = \{(v, v') \in E : v, v' \in V'\}$$
and
$$E' = E_0' \cup \bigcup_{v \in V'} E'(v).$$
If $b \in B$, then $\text{outdeg}_{G'}(b) = \text{outdeg}_G(v) \geq r$. If $v \in V' \setminus B$, then $\text{outdeg}_{G'}(v) = d' + d_B + d_C$. If $d' = d_A$, then $\text{outdeg}_{G'}(v) = d_A + d_B + d_C \geq r$. If $d' = |B| - d_B$, then $\text{outdeg}_{G'}(v) = |B| + d_C \geq |B| \geq r$. Therefore, every vertex in G' has outdegree at least r. Since $|V'| \leq n - r - 1$, the induction hypothesis implies that G' contains a cycle $\mathcal{C}'$ of length
$$\ell' \leq \frac{2|V'|}{r+1} \leq \frac{2(n-r-1)}{r+1}.$$
If (v, b) is a "new edge" in this cycle, that is, if $(v, b) \in E(v)$, then there exists $a \in A$ such that (v, a) is an edge in E, and
$$(v, a), (a, v_0), (v_0, b) \tag{1}$$
is a directed path in E. Suppose that $\mathcal{C}'$ contains exactly m new edges. Replacing every new edge (v, b) in the cycle $\mathcal{C}'$ with three old edges of the form (1), we obtain a cycle $\mathcal{C}$ in the original graph G of length
$$\ell' + 2m \leq \frac{2(n-r-1)}{r+1} + 2m.$$
The vertex v_0 occurs exactly m times in this cycle, and so the cycle decomposes into m cycles, and the sum of the lengths of these m cycles is exactly $\ell' + 2m$. This implies that G contains a cycle of length at most
$$\begin{aligned}\frac{\ell' + 2m}{m} &\leq \left(\frac{1}{m}\right)\left(\frac{2(n-r-1)}{r+1} + 2m\right) \\ &= \frac{2n}{m(r+1)} - \frac{2}{m} + 2 \\ &\leq \frac{2n}{r+1}.\end{aligned}$$
This completes the proof. □

For every real number t, let $\lceil t \rceil$ denote the smallest integer $n \geq t$.

Shen [11] obtained a significant improvement of Theorem 1. He proved that if $G = (V, E)$ is a finite directed graph with $|V| = n \geq r$ vertices such that $\text{outdeg}_G(v) \geq r$ for all $v \in V$, then G contains a cycle of length at most
$$3\left\lceil \left(\ln \frac{2+\sqrt{7}}{3}\right) \frac{n}{r} \right\rceil \approx \frac{1.312n}{r}.$$

Caccetta and Häggkvist [3] made a strong assertion about the existence of short cycles in directed graphs with many edges. Their conjecture states:

> If G is a finite directed graph with n vertices such that every vertex has outdegree at least r, then the graph contains a directed cycle of length at most $\lceil n/r \rceil$.

The *girth* of a graph is the length of the shortest cycle in the graph. We can restate the Caccetta-Häggkvist conjecture as follows: If every vertex in a finite directed graph has outdegree at least r, then the girth of the graph is at most $\lceil n/r \rceil$.

If G is a finite directed graph such that every vertex is the tail of at least one edge, that is, if $\text{outdeg}_G(v) \geq 1$ for all $v \in V$, then G contains a directed cycle. This is the case $r = 1$ of the Caccetta-Häggkvist conjecture. The conjecture has been proved for $r = 2$ by Caccetta, and Häggkvist [3], for $r = 3$ by Hamidoune [6], and for $r = 4$ and 5 by Hoáng and Reed [7]. Shen [11] proved that conjecture holds for all $r \geq 2$ and $n \geq 2r^2 - 3r + 1$. The conjecture has also been proved "up to an additive constant" in the following form: If G is a finite directed graph with n vertices such that every vertex has outdegree at least r, then the girth of G is at most $\lceil n/r \rceil + c$. Chvátal and Szemerédi [4] obtained $c = 2500$, Nishimura [9] obtained $c = 304$, and Shen [11] obtained $c = 73$.

The following example shows that the upper bound in the Caccetta-Häggkvist conjecture is best possible.

Theorem 2 (Behzad, Chartrand, and Wall [1]). *Let r be a positive integer. For every integer $n \geq r$ there is a graph $G = (V, E)$ with $|V| = n$ vertices such that $\text{outdeg}_G(v) \geq r$ for all $v \in V$ and the girth of G is exactly $\lceil n/r \rceil$.*

Proof. Let $n \geq r$ and $A = \{1, 2, \ldots, r\}$. Consider the additive group $\mathbf{Z}/n\mathbf{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$, where $\overline{x} = x + n\mathbf{Z}$. Let $G = (V, E)$ be the graph whose vertices are the congruence classes in $\mathbf{Z}/n\mathbf{Z}$ and whose edges are the ordered pairs of the form $(\overline{x}, \overline{x} + \overline{a})$, where $\overline{x} \in \mathbf{Z}/n\mathbf{Z}$ and $a \in A$. Let

$$(v_0, v_1), (v_1, v_2), \ldots, (v_{\ell-1}, v_\ell) \tag{2}$$

be a cycle of length ℓ, where $v_0 = v_\ell$ and $v_i = v_{i-1} + \overline{a_i}$ for $a_i \in A$ and $i = 1, \ldots, \ell$. Then $\overline{a_1} + \overline{a_2} + \cdots + \overline{a_\ell} = 0$ in the group $\mathbf{Z}/n\mathbf{Z}$, and so

$$a_1 + a_2 + \cdots + a_\ell \equiv 0 \pmod{n}.$$

Since

$$0 < \ell \leq a_1 + a_2 + \cdots + a_\ell \leq r\ell$$

it follows that $r\ell \geq n$ and so $\ell \geq n/r$. Therefore, $\ell \geq \lceil n/r \rceil$ and the girth of the graph G is at least $\lceil n/r \rceil$.

Conversely, let $n = \ell r - s$, where ℓ and s are integers and $0 \leq s \leq r - 1$. Then $\ell = \lceil n/r \rceil \geq 1$. If $s = 0$, let $a_i = r$ for $i = 1, \ldots, \ell$. If $1 \leq s \leq r - 1$, let $a_i = r$ for $i = 1, \ldots, \ell - 1$ and $a_\ell = r - s$. Then $a_i \in A$ for $i = 1, \ldots, \ell$ and $a_1 + a_2 + \cdots + a_\ell = n$. For any $\overline{x} \in V = \mathbf{Z}/n\mathbf{Z}$, let

$$v_i = \overline{x} + \overline{a_1} + \overline{a_2} \cdots + \overline{a_i}$$

for $i = 0, 1, \ldots, \ell$. Then (2) is a cycle in G, and the girth of G is at most $\lceil n/r \rceil$. This completes the proof. □

Exercises.

(1) Let $G = (V, E)$ be a directed graph. Prove that if $\text{outdeg}_G(v) = d^+$ for every $v \in V$ and if $\text{indeg}_G(v) = d^-$ for every $v \in V$, then $d^+ = d^-$. The graph G is called *regular of degree d* if $\text{outdeg}_G(v) = \text{indeg}_G(v) = d$ for every $v \in V$.

(2) The directed graph $G = (V, E)$ is *path-connected* if for every pair of distinct vertices $v, v' \in V$ there is a directed path from v to v'. If G is path-connected, then the *distance* from vertex v to vertex v' is the length of the shortest directed path from v to v'. The *diameter* of a path-connected graph G is the maximum distance between two vertices of G. Prove that if G is a path-connected directed graph with diameter D and girth g, then $g \leq D + 1$.

(3) Let $G = (V, E)$ be a finite directed graph with neither loops nor digons. For every vertex $v \in V$, the *first neighborhood* $N^+(v)$ consists of all vertices v' such that $(v, v') \in E$. The *second neghborhood* $N^{++}(v)$ is the set of all vertices $v'' \in V$ such that (i) there is a vertex $v' \in N^+(v)$ with $(v, v') \in E$ and $(v', v'') \in E$, and (ii) $v'' \notin N^+(v)$. Seymour's *second neighborhood conjecture* states that there is a vertex $v \in V$ such that

$$|N^+(v)| \leq |N^{++}(v)|.$$

Show that the second neighborhood conjecture implies that if G is a graph with n vertices such that (i) G contains no loops and no digons and (ii) every vertex of G has indegree and outdegree at least $n/3$, then the Caccetta-Häggkvist conjecture is true for G, that is, G contains a directed triangle. (Hint: Prove that there is a vertex $v \in V$ such that $(v'', v) \in E$ for some $v'' \in N^{++}(v)$.)

2. Directed triangles in directed graphs

An equivalent form of the Caccetta-Häggkvist conjecture is the following: If G is a finite directed graph with n vertices such that every vertex has outdegree at least n/k, then G contains a directed cycle of length at most k. If $k = 1$, then every vertex has degree n, so the graph contains loops, which are cycles of length 1.

Theorem 3 (Caccetta, and Häggkvist [3]). *If G is a finite directed graph with n vertices such that every vertex has outdegree at least $n/2$, then G contains a loop or a digon, that is, a directed cycle of length at most 2.*

Proof. Suppose that every vertex of G has outdegree at least $n/2$. By Lemma 1, there exists a vertex $v_0 \in V$ such that $\mathrm{indeg}_G(v_0) \geq n/2$. Let $V' = \{v' \in V : (v', v_0) \in E\}$ and let $V'' = \{v'' \in V : (v_0, v'') \in E\}$. Since $|V'| \geq n/2$ and $|V''| \geq n/2$, it follows that the sets V', V'', and $\{v_0\}$ cannot be pairwise disjoint. If $v_0 \in V' \cup V''$, then G contains a loop. Otherwise, $V' \cap V'' \neq \emptyset$, and G contains a digon. □

For $k = 3$, the Caccetta-Häggkvist conjecture asserts that if G has outdegree at least $n/3$, then G contains a cycle of length at most 3, that is, a loop, digon, or triangle. This is a famous unsolved problem in graph theory.

Theorem 4 (Caccetta, and Häggkvist [3]). *Let*

$$c_0 = \frac{3 - \sqrt{5}}{2} \approx 0.3820\ldots.$$

If $G = (V, E)$ is a finite directed graph with $|V| = n$ vertices such that $\mathrm{outdeg}_G(v) \geq c_0 n$ for all $v \in V$, then G contains a cycle of length at most 3.

Proof. Let $0 < c < 1$, and let $G = (V, E)$ be a directed graph with n vertices such that $\text{outdeg}_G(v) \geq cn$ for all $v \in V$ and G does not contain a loop, digon, or triangle. We shall prove that $c < (3 - \sqrt{5})/2$.

By Lemma 1, the graph G contains a vertex v_0 such that $\text{indeg}_G(v_0) \geq cn$. Let A be the set of vertices a such that $(a, v_0) \in E$, and let B be the set of vertices b such that $(v_0, b) \in E$. Then $|A| \geq cn$ and $|B| \geq cn$. If $v_0 \in A \cup B$, then G contains a loop. Similarly, if $v_0 \notin A \cup B$ and $A \cap B \neq \emptyset$, then G contains a digon. Therefore, we can assume that the sets A, B and $\{v_0\}$ are pairwise disjoint.

Let G' be the complete subgraph of G induced by B, that is, G' is the graph whose vertex set is B and whose edges are all ordered pairs (b, b') such that $b, b' \in B$ and $(b, b') \in E$. Since $|B| < n$, it follows from the induction hypothesis that if $\text{outdeg}_{G'}(b) \geq c|B|$ for all $b \in B$, then the graph G' contains a triangle, and so G contains a triangle. Therefore, we can assume that there is a vertex $b_0 \in B$ such that $\text{outdeg}_{G'}(b_0) < c|B|$. Let W be the set of all vertices $w \in V \setminus B$ such that $(b_0, w) \in E$. Since $\text{outdeg}_G(b_0) \geq cn$, it follows that

$$|W| = \text{outdeg}_G(b_0) - \text{outdeg}_{G'}(b_0) > cn - c|B|.$$

If $v_0 \in W$, then G contains a digon. If $A \cap W \neq \emptyset$, then G contains a triangle. Therefore, we can assume that the sets A, B, W, and $\{v_0\}$ are pairwise disjoint subsets of V, and so

$$n \geq |A| + |B| + |W| + 1 > 2cn + (1 - c)|B| + 1 > 3cn - c^2.$$

This implies that

$$c^2 - 3c + 1 > 0$$

and so

$$c < \frac{3 - \sqrt{5}}{2}.$$

Therefore, if $c \geq (3 - \sqrt{5})/2$, then G contains a cycle of length at most 3. □

The constant c in Theorem 4 has been reduced by Bondy [2], who obtained

$$c_0 = \frac{2\sqrt{6} - 3}{5} \approx 0.3798$$

and by Shen [10], who obtained

$$c_0 = 3 - \sqrt{7} = 0.3542 \ldots.$$

3. Kemperman's theorem for nonabelian groups

In the following sections we shall prove the Caccetta-Häggkvist conjecture for two important classes of finite directed graphs: Cayley graphs and vertex-transitive graphs. The proof depends on a result of Kemperman that gives an upper bound for the growth of certain subsets of a group.

Let Γ be a finite group, written multiplicatively, and let (A, B) be a pair of finite subsets of Γ. The *product set* $A \cdot B$ is the set

$$A \cdot B = \{ab : a \in A \text{ and } b \in B\}.$$

We define the iterated product sets $B^2 = B \cdot B$ and $B^k = B \cdot B^{k-1}$ for all $k \geq 2$. Then

$$B^k = \{b_1 b_2 \cdots b_k : b_i \in B \text{ for } i = 1, 2, \ldots, k\}.$$

We usually write AB instead of $A \cdot B$. For $x \in \Gamma$ and $A \subseteq \Gamma$, let

$$Ax = A\{x\} = \{ax : a \in A\}$$

and

$$xA = \{x\}A = \{xa : a \in A\}.$$

Let $|X|$ denote the cardinality of the set X. For any pair (A, B) of finite subsets of Γ, we define

$$k(A, B) = |A| + |B| - |A + B|.$$

Theorem 5 (Kemperman [8])**.** *Let Γ be a finite group and let (A, B) be a pair of finite subsets of Γ such that*

(i) $1 \in A \cap B$

(ii) *If $a \in A$, $b \in B$, and $ab = 1$, then $a = b = 1$.*

Then

$$|AB| \geq |A| + |B| - 1.$$

Proof. Suppose there exist pairs (A, B) of subsets of Γ such that A and B satisfy conditions (i) and (ii), but $|AB| < |A| + |B| - 1$. Equivalently,

$$k(A, B) = |A| + |B| - |AB| \geq 2. \tag{3}$$

Consider pairs (A, B) that have the maximum value of $k(A, B)$. Among all such pairs, choose (A, B) with the minimum value of $|A|$.

Since $1 \in A \cap B$, it follows that $AB \supseteq A \cup B$. If $A \cap B = \{1\}$, then $|AB| \geq |A \cup B| = |A| + |B| - 1$, which contradicts (3). Therefore, there exists $x \in A \cap B$ with $x \neq 1$. We introduce the sets

$$\begin{aligned} A_1 &= Ax^{-1} \cap A \\ B_1 &= xB \cup B \\ A_2 &= Ax \cup A \\ B_2 &= x^{-1}B \cap B. \end{aligned}$$

Then

$$A_1B_1 \subseteq AB \text{ and } A_2B_2 \subseteq AB.$$

We shall show that A_1 is a proper subset of A. Note that $x \in A$. If $x^k \in A$ for all positive integers k, then x has finite order m since A is finite, and so $x^{m-1} = x^{-1} \in A$. Since $x \in B$, we have $1 = x^{-1} \cdot x \in AB$ and so $x = 1$, which is a contradiction. It follows that there must exist a largest positive integer k such that $x^k \in A$. If $x^k \in A_1$, then $x^k \in Ax^{-1}$ and so $x^{k+1} \in A$, which is a contradiction. Therefore, $x^k \in A \backslash A_1$ and $|A_1| < |A|$.

By Exercise 1,

$$A_1x = (Ax^{-1} \cap A)x = A \cap Ax$$

and so

$$|A_1| = |A_1x| = |A \cap Ax|$$

and

$$|A_1| + |A_2| = |A \cap Ax| + |Ax \cup A| = |A| + |Ax| = 2|A|. \tag{4}$$

Similarly,

$$|B_1| + |B_2| = 2|B|. \tag{5}$$

Adding (4) and (5), we obtain

$$(|A_1| + |B_1|) + (|A_2| + |B_2|) = 2(|A| + |B|). \tag{6}$$

We shall show that the pairs (A_1, B_1) and (A_2, B_2) also satisfy conditions (i) and (ii). Since $1 \in A \cap B$ and $x \in A \cap B$, it follows that

$$1 \in A_1 \cap B_1 \text{ and } 1 \in A_2 \cap B_2$$

and so the first condition is satisfied.

Suppose that $a_1 \in A_1$, $b_1 \in B_1$, and $a_1 b_1 = 1$. Then $b_1 \in B$ or $b_1 \in xB$. If $b_1 \in B$, then $a_1 \in A_1 = Ax^{-1} \cap A \subseteq A$ implies that $a_1 = b_1 = 1$. On the other hand, if $b_1 \in xB$, then $b_1 = xb$ for some $b \in B$. Since $a_1 \in A_1 \subseteq Ax^{-1}$, there exists $a \in A$ such that $a_1 = ax^{-1}$. Then $1 = a_1 b_1 = ax^{-1}xb = ab$, and so $a = b = 1$. It follows that $a_1 = x^{-1} \in A$, which is impossible because $x \in B$ and $x \neq 1$. Therefore, the pair (A_1, B_1) satisfies condition (ii). Similarly, (A_2, B_2) satisfies condition (ii).

By the maximality of $k(A, B)$,

$$|A_1| + |B_1| - |A_1 B_1| = k(A_1, B_1) \leq k(A, B) = |A| + |B| - |AB| \tag{7}$$

and

$$|A_2| + |B_2| - |A_2 B_2| = k(A_2, B_2) \leq k(A, B) = |A| + |B| - |AB|. \tag{8}$$

Adding and rearranging (7) and (8), we obtain

$$2|AB| \leq |A_1 B_1| + |A_2 B_2|.$$

Since $A_1 B_1 \subseteq AB$, $A_2 B_2 \subseteq AB$, we also have

$$|A_1 B_1| \leq |AB| \text{ and } |A_2 B_2| \leq |AB|$$

and so

$$|A_1 B_1| = |A_2 B_2| = |AB|.$$

Therefore,

$$k(A_1, B_1) + k(A_2, B_2) = 2k(A, B).$$

The maximality of $k(A, B)$ implies that

$$k(A_1, B_1) = k(A_2, B_2) = k(A, B)$$

but this is impossible since the inequality $|A_1| < |A|$ contradicts the minimality of $|A|$. This completes the proof. □

Theorem 6. *Let Γ be a group and let B be a finite subset of Γ with $1 \in B$. If the only solution of the equation $b_1 b_2 \cdots b_k = 1$ with $b_i \in B$ for all $i = 1, \ldots, k$ is $b_1 = b_2 = \cdots = b_k = 1$, then*

$$|B^k| \geq k|B| - k + 1.$$

Proof. Exercise 2. □

Exercises.

(1) Let A be a finite subset of a group Γ and let $x \in \Gamma$. Prove that $(Ax^{-1} \cap A)x = A \cap Ax$.
(2) Prove Theorem 6 by induction on k.

4. The Caccetta-Häggkvist conjecture for Cayley graphs

Let Γ be a finite group, not necessarily abelian. We write the group operation multiplicatively. Let A be a subset of Γ. The *Cayley graph* Cayley(Γ, A) is the graph whose vertex set is the group Γ, and whose edge set consists of all ordered pairs of form (v, va), where $v \in \Gamma$ and $a \in A$. By Exercise 2, every vertex in Cayley(Γ, A) has outdegree $|A|$ and indegree $|A|$. Moreover, Cayley(Γ, A) contains a loop if and only if $1 \in A$, and Cayley(Γ, A) contains a digon if and only if $\{a, a^{-1}\} \subseteq A$ for some $a \in \Gamma, a \neq 1$.

Lemma 2. *Let Γ be a finite group and $A \subseteq \Gamma$. The graph Cayley(Γ, A) contains a directed cycle of length ℓ if and only if $1 \in A^{\ell}$.*

Proof. If $1 \in A^{\ell}$, then there exist $a_1, a_2, \ldots, a_{\ell}$ in A such that $a_1 a_2 \cdots a_{\ell} = 1$. For any $v_0 \in \Gamma$, if we define

$$v_i = v_{i-1} a_i = v_0 a_1 a_2 \cdots a_i$$

for $i = 1, \ldots, \ell$, then $v_{\ell} = v_0$ and

$$(v_0, v_1), (v_1, v_2), \ldots, (v_{\ell-1}, v_{\ell}) \tag{9}$$

is a directed cycle of length ℓ in Cayley(Γ, A).

Conversely, if (9) is a directed cycle in Γ, then $v_0 \in \Gamma$ and there exist $a_1,\ldots,a_{\ell} \in A$ such that $v_i = v_{i-1} a_i$ for $i = 1, \ldots, \ell$. This implies that if $1 \leq i < j \leq \ell$, then

$$v_j = v_{i-1} a_i a_{i+1} \cdots a_j.$$

In particular,

$$v_0 = v_{\ell} = v_0 a_1 a_2 \cdots a_{\ell}$$

and so

$$1 = a_1 \cdots a_{\ell} \in A^{\ell}.$$

This completes the proof. □

Theorem 7 (Hamidoune [5])**.** *Let Γ be a finite group of order n, and let A be a subset of Γ such that $|A| \geq n/k$. Then the graph Cayley(Γ, A) contains a cycle of length at most k.*

Proof. If every cycle in the graph Cayley(Γ, A) has length greater than k, then Lemma 2 implies that

$$1 \notin A \cup A^2 \cup \cdots \cup A^k.$$

Let $B = A \cup \{1\}$. Then $|B| = |A| + 1$. Since the only solution of $1 = b_1 b_2 \cdots b_k \in B^k$ is $b_1 = b_2 = \cdots = b_k = 1$, it follows from Theorem 6 that

$$n = |\Gamma| \geq |B|^k \geq k|B| - k + 1 = k|A| + 1 > k|A|$$

and so $|A| < n/k$, which is false. Thus, Cayley(Γ, A) must contain a cycle of length at most k. □

Exercises.

(1) Prove that the Cayley graph Cayley(Γ, A) is path-connected if and only if the semigroup generated by A is Γ.
(2) Prove that if x is a vertex in the graph Cayley(Γ, A), then $\mathrm{indeg}_G(x) = \mathrm{outdeg}_G(x) = |A|$.

(3) The sequence of edges (9) is a *simple directed cycle* in Γ if $v_i \neq v_j$ for $0 \leq i < j \leq \ell - 1$. Prove that $\mathrm{Cayley}(\Gamma, A)$ contains a simple directed cycle of length ℓ if and only if there exists a sequence of elements $a_1, \ldots, a_\ell$ in A such that $a_i a_{i+1} \cdots a_j = 1$ for $1 \leq i \leq j \leq \ell$ if and only if $i = 0$ and $j = \ell$.

(4) Let $\Gamma = \langle x \rangle$ be the cyclic group of order $d(g-1)+1$, written multiplicatively, and let $A = \{x, x^2, \ldots, x^d\}$. Prove that the graph $\mathrm{Cayley}(\Gamma, A)$ is regular of degree d with girth g.

5. Graph automorphisms and vertex-transitive graphs

Let $G = (V, E)$ and $G' = (V', E')$ be finite directed graphs. The function $x : V \to V'$ is a *graph isomorphism* if x is a bijection and $(v_1, v_2) \in E$ if and only if $(x(v_1), x(v_2)) \in E'$. A *graph automorphism* is a graph isomorphism from G to G. The automorphisms of a graph form a group, denoted $\mathrm{Aut}(G)$. We denote the action of an automorphism $x : V \to V$ on the vertex v by xv.

Let Γ be a group of graph automorphisms of G, that is, a subgroup of $\mathrm{Aut}(G)$. The graph G is called *vertex-transitive with respect to* Γ if, for every pair of vertices $v, v' \in V$, there is an automorphism $x \in \Gamma$ such that $xv = v'$. We call G *vertex-transitive* if it is vertex-transitive with respect to some group of automorphisms. In a vertex-transitive graph, $\mathrm{outdeg}_G(v) = \mathrm{outdeg}_G(v')$ for all vertices $v, v' \in V$ (Exercise 1).

For example, every Cayley graph is vertex-transitive. Let $G = \mathrm{Cayley}(\Gamma, A)$, where Γ is a finite group and $A \subseteq \Gamma$. To every element $x \in \Gamma$ there is a bijection $x : \Gamma \to \Gamma$ defined by $v \mapsto xv$ for all $v \in \Gamma$. If (v_1, v_2) is an edge in G, then $v_2 = v_1 a$ for some $a \in A$, and $(xv_1, xv_2) = (xv_1, (xv_1)a)$ is also an edge in G. Thus, the map $x \mapsto xv$ is an automorphism of G. In particular, if $v, v' \in \Gamma$ and $x = v'v^{-1}$, then the map $w \mapsto xw = v'v^{-1}w$ sends v to v', and so $\mathrm{Aut}(G)$ acts transitively on Γ.

We shall prove that the Caccetta-Häggkvist conjecture is true for all vertex-transitive graphs.

Theorem 8 (Hamidoune [5])**.** *Let G be a vertex-transitive finite directed graph with n vertices such that $\mathrm{outdeg}_G(v) = d$ for every vertex v of G. Then G contains a cycle of length at most $\lceil n/d \rceil$.*

Proof. Let Γ be a group of automorphisms that acts transitively on the set V of vertices of a finite directed graph G. For every vertex $v \in V$, the *stabilizer of* v is the set

$$H_v = \{x \in \Gamma : xv = v\}.$$

H_v is a subgroup of Γ.

Choose a vertex $v_0 \in V$, and let $H_0 = H_{v_0}$. Since G is vertex-transitive, there is a set $\{x_v\}_{v \in V}$ contained in Γ such that $x_v v_0 = v$ for all $v \in V$. Then

$$\begin{aligned} H_v &= \{x \in \Gamma : xv = v\} \\ &= \{x \in \Gamma : x x_v v_0 = x_v v_0\} \\ &= \{x \in \Gamma : x_v^{-1} x x_v v_0 = v_0\} \\ &= \{x \in \Gamma : x_v^{-1} x x_v \in H_0\} \\ &= x_v H_0 x_v^{-1}. \end{aligned}$$

The subgroup H_0 is normal in Γ if and only if $H_v = H_0$ for all $v \in V$.

For all $x \in \Gamma$, we have $xv_0 = v$ if and only if $xv_0 = x_v v_0$ if and only if $x_v^{-1}x \in H_0$ if and only if $x \in x_v H_0$. Therefore,

$$x_v H_0 = xH_0 = \{x \in \Gamma : xv_0 = v\}.$$

Let

$$\Gamma_0 = \Gamma/H_0 = \{xH_0 : x \in \Gamma\}$$

denote the set of left cosets of H_0. The map $\phi : V \to \Gamma/H_0$ defined by $v \mapsto x_v H_0$ is a one-to-one correspondence between the vertices of G and the left cosets of H_0, and so

$$|\Gamma_0| = |\Gamma/H_0| = |V| = n$$

and

$$|\Gamma| = |\Gamma/H_0||H_0| = n|H_0|.$$

We can use the left cosets of H_0 to describe the edges in the graph G. Let

$$A = \{x \in \Gamma : (v_0, xv_0) \in E\}.$$

If $x \in A$ and $h \in H_0$, then $(v_0, xhv_0) = (v_0, xv_0) \in E$ and so $xh \in A$, hence $xH_0 \subseteq A$. It follows that A is a union of left cosets of H_0. Let

$$A_0 = \{xH_0 : xH_0 \subseteq A\} = \{xH_0 : (v_0, xv_0) \in E\} = \{x_v H_0 : (v_0, v) \in E\}.$$

Then

$$|A_0| = \mathrm{outdeg}_G(v_0) = d$$

and

$$|A| = |A_0||H_0| = d|H_0|.$$

Since Γ is a group of automorphisms of the graph G, the ordered pair (v, v') is an edge of G if and only if $(x_v^{-1}v, x_v^{-1}v') = (v_0, x_v^{-1}x_{v'}v_0) \in E$. Thus,

$$(v, v') \in E \text{ if and only if } x_v^{-1}x_{v'}H_0 \in A_0.$$

Suppose that H_0 is a normal subgroup of Γ. Then Γ_0 is a group of order n. The graph $\mathrm{Cayley}(\Gamma_0, A_0)$ has $|\Gamma_0| = n$ vertices and $|A_0| = d$ edges. By Theorem 7, $\mathrm{Cayley}(\Gamma_0, A_0)$ contains a cycle of length not exceeding $\lceil n/|A_0|\rceil = \lceil n/d\rceil$.

We shall show that the graphs G and $\mathrm{Cayley}(\Gamma_0, A_0)$ are isomorphic. Recall the bijection $\phi : V \to \Gamma_0$ defined by $\phi(v) = x_v H_0$. Let $(v, v') \in E$, and define $x = x_v^{-1}x_{v'}$. Then $xH_0 = x_v^{-1}x_{v'}H_0 \in A_0$ and $(x_v H_0)(xH_0) = x_{v'}H_0$, hence $(\phi(v), \phi(v')) = (x_v H_0, x_{v'}H_0)$ is an edge in $\mathrm{Cayley}(\Gamma_0, A_0)$. Conversely, if $(\phi(v), \phi(v')) = (x_v H_0, x_{v'}H_0)$ is an edge in $\mathrm{Cayley}(\Gamma_0, A_0)$, then there is a coset $xH_0 \in A_0$ such that $x_v H_0 xH_0 = x_v xH_0 = x_{v'}H_0$. It follows that $x_v^{-1}x_{v'}H_0 \in A_0$ and so $(v, v') \in E$. Thus, the map $\phi : V \to \Gamma_0/H_0$ is a graph isomorphism, and so G contains a cycle of length at most n/d.

Next we consider the general case when H_0 is not necessarily a normal subgroup of Γ. The Cayley graph $\mathrm{Cayley}(\Gamma, A)$ contains $|\Gamma| = n|H_0|$ vertices, and and the outdegree of every vertex is $|A| = d|H_0|$. By Theorem 7, $\mathrm{Cayley}(\Gamma, A)$ has a cycle of length ℓ, where

$$\ell \leq \left\lceil \frac{|\Gamma_0|}{|A|} \right\rceil = \left\lceil \frac{n|H_0|}{d|H_0|} \right\rceil = \left\lceil \frac{n}{d} \right\rceil.$$

By Lemma 2, there exist elements $a_1, \ldots, a_\ell \in A$ such that

$$a_1 a_2 \cdots a_{\ell-1} a_\ell = 1.$$

Let $v_0 \in \Gamma$ and consider the sequence of vertices $v_0, v_1, \ldots, v_\ell$, where

$$v_i = a_1 a_2 \cdots a_i v_0$$

for $i = 1, 2, \ldots, \ell$. Then $(v_0, a_i v_0) \in E$ since $a_i \in A$ for $i = 1, 2, \ldots, \ell$. Since Γ is a group of graph automorphisms, we have

$$(v_{i-1}, v_i) = ((a_1 a_2 \cdots a_{i-1})v_0, (a_1 a_2 \cdots a_{i-1})a_i v_0) \in E \text{ for } i = 1, 2, \ldots, \ell$$

and

$$v_\ell = a_1 a_2 \cdots a_{\ell-1} a_\ell v_0 = 1 \cdot v_0 = v_0.$$

It follows that

$$(v_0, v_1), (v_1, v_2), \ldots, (v_{\ell-1}, v_\ell) = (v_{\ell-1}, v_0)$$

is a cycle in G of length $\ell \leq \lceil n/d \rceil$. This completes the proof. □

Exercise.

(1) If $G = (V, E)$ is a vertex-transitive graph, then there is an integer d such that G is regular of degree d, that is, $\mathrm{outdeg}_G(v) = \mathrm{indeg}_G(v) = d$ for all $v \in V$.

6. Additive compression

Let V_1 and V_2 be finite disjoint sets with $|V_1| = n_1$ and $|V_2| = n_2$, and let $E \subseteq V_1 \times V_2$. The graph $G = (V_1 \cup V_2, E)$ is called a *bipartite graph.* Every edge in G has its tail in V_1 and its head in V_2, and so

$$d_1 = \max\{\mathrm{outdeg}_G(v_1) : v_1 \in V_1\} \leq n_2$$

and

$$d_2 = \max\{\mathrm{indeg}_G(v_2) : v_2 \in V_2\} \leq n_1.$$

Let $\alpha : V_1 \to \Gamma$ and $\beta : V_2 \to \Gamma$ be one-to-one functions from the vertices of G to a group Γ. We define

$$\alpha(V_1) \stackrel{G}{+} \beta(V_2) = \{\alpha(v_1) + \beta(v_2) : (v_1, v_2) \in E\}.$$

For all bipartite graphs G, we have

$$|\alpha(V_1) \stackrel{G}{+} \beta(V_2)| \geq \max(d_1, d_2) \tag{10}$$

for every group Γ and all one-to-one maps $\alpha : V_1 \to \Gamma$ and $\beta : V_2 \to \Gamma$.

Consider the *complete bipartite graph* $K_{n_1,n_2} = (V_1 \cup V_2, V_1 \times V_2)$. We have $d_1 = \mathrm{outdeg}_G(v_1) = n_2$ for all $v_1 \in V_1$ and $d_2 = \mathrm{indeg}_G(v_2) = n_1$ for all $v_2 \in V_2$. If $\Gamma = \mathbf{Z}$ and $\alpha : V_1 \to \Gamma$ and $\beta : V_2 \to \Gamma$ are one-to-one functions, then $|\alpha(V_1) \stackrel{G}{+} \beta(V_2)| \geq d_1 + d_2 - 1$. If p is a prime and $\Gamma = \mathbf{Z}/p\mathbf{Z}$, then the Cauchy-Davenport theorem states that $|\alpha(V_1) \stackrel{G}{+} \beta(V_2)| \geq \min(d_1 + d_2 - 1, p)$. In particular, if $\max(d_1, d_2) \leq p - 1$ and $\min(d_1, d_2) \geq 2$, then $|\alpha(V_1) \stackrel{G}{+} \beta(V_2)| \geq \max(d_1, d_2) + 1$. One might guess that this is always a lower bound for $|\alpha(V_1) \stackrel{G}{+} \beta(V_2)|$, but the following beautiful construction by Josh Greene shows that inequality (10) is best possible.

Let A and B be finite subsets of an abelian group Γ. For every $x \in \Gamma$, we define the *representation function*

$$r_{A,B}(x) = |\{(a, b) \in A \times B : a + b = x\}|.$$

We construct the bipartite graph $G = (V_1 \cup V_2, E)$, where

$$V_1 = -A$$

$$V_2 = A + B$$

and

$$E = \{(-a, a+b) : b \in B\}.$$

For all $v_1 \in V_1$ and $v_2 \in V_2$ we have

$$\mathrm{outdeg}_G(v_1) = |B|$$

and

$$\mathrm{indeg}_G(v_2) = r_{A,B}(v_2).$$

Then

$$d_1 = \max\{\mathrm{outdeg}_G(v_1) : v_1 \in V_1\} = |B|$$

and

$$d_2 = \max\{\mathrm{indeg}_G(v_2) : v_2 \in V_2\} = \max\{r_{A,B}(x) : x \in A+B\} \leq |B|.$$

Define $\alpha : V_1 \to \Gamma$ by $\alpha(v_1) = v_1$ and $\beta : V_2 \to \Gamma$ by $\beta(v_2) = v_2$. Then

$$\alpha(V_1) \overset{G}{+} \beta(V_2) = B$$

and

$$|\alpha(V_1) \overset{G}{+} \beta(V_2)| = |B| = \max(d_1, d_2).$$

Greene applied his construction in the following case. Consider the Fermat prime $p = 257 = 2^{2^3} + 1$ and the finite field $\Gamma = \mathbf{Z}/257\mathbf{Z}$. Let

$$A = B = \{0\} \cup \{\pm 2^i : i = 0, 1, \ldots, 7\} \subseteq \mathbf{Z}/257\mathbf{Z}$$

and

$$A + A = \{a + a' : a, a' \in a\} \subseteq \mathbf{Z}/257\mathbf{Z}.$$

Then $|A| = 17$ and $|A+A| = 105$. Note that every element of $A+A$ can be written as the sum of two distinct elements of A, since $0+0 = 1+(-1)$, $2^7+2^7 = 0+(-1)$, and $2^i + 2^i = 0 + 2^{i+1}$ for $i = 0, 1, \ldots, 6$. Therefore, $r_{A,A}(x) \geq 2$ for all $x \in A+A$, and so $d_1 = 105$ and $d_2 \geq 2$.

We conclude with a nice application of Sidon sets. A *Sidon set* is a subset A of an abelian group such that every element of $A+A$ has a unique representation as the sum of two elements of A. Equivalently, $r_{A,A}(x) = 1$ for all $x \in A+A$.

Let $G = (V, E)$ be an undirected graph, and let $\alpha : V \to \Gamma$ and $\gamma : E \to \Gamma$ be one-to-one functions from the vertices and edges of G into a group Γ. Consider the set $\{\alpha(v) + \gamma(e) : v \in e\}$. If the maximum degree of a vertex in V is n, then $|\{\alpha(v) + \gamma(e) : v \in e\}| \geq n$.

Theorem 9 (Jacob Fox). *Let K_n denote the complete graph on n vertices. There are one-to-one functions $\alpha : V \to \mathbf{Z}$ and $\gamma : E \to \mathbf{Z}$ such that $|\{\alpha(v) + \gamma(e) : v \in e\}| = n$.*

Proof. Denote the vertices of K_n by $V = \{v_1, \ldots, v_n\}$ and the edges of G by $E = \{e_{i,j} = \{v_i, v_j\} : i, j = 1, \ldots, n\}$. Let $A = \{a_1, \ldots, a_n\}$ be a Sidon set, and define the functions α and γ by $\alpha(v_i) = -a_i$ for $i = 1, \ldots, n$ and $\gamma(e_{i,j}) = a_i + a_j$ for $i, j = 1, \ldots, n$. Then $\{\alpha(v) + \gamma(e) : v \in e\} = A$. This completes the proof. □

References

[1] Mehdi Behzad, Gary Chartrand, and Curtiss E. Wall, *On minimal regular digraphs with given girth*, Fund. Math. **69** (1970), 227–231.

[2] J. A. Bondy, *Counting subgraphs: a new approach to the Caccetta-Häggkvist conjecture*, Discrete Math. **165/166** (1997), 71–80, Graphs and combinatorics (Marseille, 1995).

[3] Louis Caccetta and R. Häggkvist, *On minimal digraphs with given girth*, Proceedings of the Ninth Southeastern Conference on Combinatorics, Graph Theory, and Computing (Florida Atlantic Univ., Boca Raton, Fla., 1978) (Winnipeg, Man.), Congress. Numer., XXI, Utilitas Math., 1978, pp. 181–187.

[4] V. Chvátal and E. Szemerédi, *Short cycles in directed graphs*, J. Combin. Theory Ser. B **35** (1983), no. 3, 323–327.

[5] Yahya Ould Hamidoune, *An application of connectivity theory in graphs to factorizations of elements in groups*, European J. Combin. **2** (1981), no. 4, 349–355.

[6] ———, *A note on minimal directed graphs with given girth*, J. Combin. Theory Ser. B **43** (1987), no. 3, 343–348.

[7] C. T. Hoàng and B. Reed, *A note on short cycles in digraphs*, Discrete Math. **66** (1987), no. 1-2, 103–107.

[8] J. H. B. Kemperman, *On complexes in a semigroup*, Nederl. Akad. Wetensch. Proc. Ser. A. **59** = Indag. Math. **18** (1956), 247–254.

[9] Tsuyoshi Nishimura, *Short cycles in digraphs*, Proceedings of the First Japan Conference on Graph Theory and Applications (Hakone, 1986), vol. 72, 1988, pp. 295–298.

[10] Jian Shen, *Directed triangles in digraphs*, J. Combin. Theory Ser. B **74** (1998), no. 2, 405–407.

[11] ———, *On the girth of digraphs*, Discrete Math. **211** (2000), no. 1-3, 167–181.

Department of Mathematics, Lehman College (CUNY), Bronx, New York 10468
E-mail address: melvyn.nathanson@lehman.cuny.edu